REMARKS/ARGUMENTS

This Amendment is in response to the Office Action dated August 10, 2005. Claims 1-41 are pending. Claims 1-41 are rejected. Claims 1-2, 6-7, 12, 18-22, 26-27, 32, and 37-41 have been amended. No claims have been canceled or added. Accordingly, claims 1-41 remain pending in the present application.

Claims 6 and 26 have been amended to correct typographical errors.

Claims 1, 21, and 41 are rejected under 35 USC 102(e) as being anticipated by Johnson (6,898,577). Claims 2-20, 22-40 are rejected under 35 USC 103(a) as being unpatentable over Johnson in view of Thompson (6,725,382). Applicant respectfully disagrees as to the claims as amended.

The present invention provides a method for providing security in password-based access to computer networks, the network including a server and a remote user, comprising the steps of: (a) signing a phrase by a security chip of the server using an encryption key, *wherein the encryption key is known only to the security chip*; (b) associating the signed phrase with the remote user; (c) signing the phrase with the encryption key obtained by the security chip when a request for access to the computer network is received from the remote user; (d) comparing the phrase signed with the obtained encryption key with the signed phrase associated with the remote user; and (e) granting access to the remote user if the phrase signed with the obtained encryption key is the same as the stored signed phrase associated with the remote user.

With the present invention, it is the encryption key itself which contains the entropy, not the phrase which is encrypted. It is the comparison of the effects of the encryption key (in signing the phrase), not the comparison of the phrase itself that determines access. This entropy is provided by the fact that the encryption key is known only to the security chip. An example security chip is a Trusted Platform Module (TPM), which follows the Trusted Computing Platform Alliance

(TCPA) protocols.

In contrast, neither Johnson nor Thompson discloses a security mechanism which uses the entropy of the encryption key to determine access, where the encryption key is known only to a security chip. Johnson discloses a bank receiving a password encrypted with a first encryption scheme from a customer, which the bank's server decrypts. The bank's server then re-encrypts the password with a second encryption scheme and compares it with a stored encrypted password for the customer. Thompson discloses prompts a user for a password upon a boot of a PC. The password is then encrypted with a stored key and compared with a stored password. In both Johnson and Thompson, the entropy is provided by the passwords, not by the encryption keys. Neither reference discloses the use of a security chip nor discloses encryption keys which are known only to the security chip, and using the entropy provided by such an encryption key to determine access.

Thus, neither Johnson nor Johnson in view of Thompson teaches the present invention as recited in claims 1-41. Applicant therefore submits that claims 1-41 are patentable over the cited references and respectfully requests reconsideration and allowance of the claims as now presented.

The prior art made of record and not relied upon has been reviewed and does not appear to be any more relevant than the applied references.

Applicants' attorney believes this application in condition for allowance. Should any unresolved issues remain, Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,
SAWYER LAW GROUP LLP

October 28, 2005
Date

/Michele Liu/ Reg. No. 44,875
Michele Liu
Attorney for Applicant(s)
(650) 493-4540